TESTIMONY OF
THE HONORABLE STEVE LARGENT
PRESIDENT AND CHIEF EXECUTIVE OFFICER
CTIA – THE WIRELESS ASSOCIATON®

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

FEBRUARY 1, 2006

Chairman Barton, Ranking Member Dingell and members of the Committee, thank you for the opportunity to appear before you this afternoon to testify on the theft and illegal sale of phone records by data brokers. At the outset of my testimony, I want to make it unequivocally clear that the wireless industry, and more specifically, the wireless carriers that I represent take this matter very seriously. The theft of this data is unacceptable, and CTIA and wireless carriers believe that the current practice of "pretexting" is illegal. Chairwoman Majoras has declared that the Federal Trade Commission currently has the authority it needs to prosecute these thieves. Carriers have successfully filed injunctions to take these sites down. Additionally, CTIA and the wireless industry are on record as supporting Congress's efforts to enact federal legislation that criminalizes the fraudulent behavior by third parties to obtain, sell or distribute call records. I believe that it is important to note that the four national carriers: Verizon Wireless, Cingular, Sprint Nextel, and T-Mobile have all filed complaints and obtained injunctions across the country to shut these data thieves down.

The fact that data brokers apparently have been able to break and enter carrier customer service operations to obtain call records has given our industry a black eye. To quote from one of CTIA's member companies' Code of Conduct, "Great companies are defined by their reputation for ethics and integrity in every aspect of their business. By their actions, these companies demonstrate the values that serve as the foundation of their culture and attract the best customers, employees and stakeholders in their industry." The wireless industry is dedicated to being responsive to its customers' requests for assistance with their service because of its concern for wireless customers. To the extent that the theft of customer call records has jeopardized the industry's reputation, I believe this is most unfortunate because trust is a currency that is difficult to refund.

PRETEXTING

Overwhelmingly, the vast majority of cell phone records are being fraudulently obtained through the use of "pretexting," which is nothing more than lying to obtain something you aren't entitled to procure lawfully. Allow me to explain how these data thieves operate. For the sake of illustration, if someone -- and in most cases it appears to be a private investigator – wants to acquire my call records, the private investigator will go to a website that publicly offers to obtain such records such as locatecell.com. The person trying to obtain my call records will provide the website in most cases with nothing more than my name and phone number. At that point, the website or a subcontractor of the website will pose as *Steve Largent* and call a carrier's customer service department to get the records.

Customer Service Representatives (CSR) are trained to require more than just a name and phone number, but the thieves are well trained too and often badger, threaten or plead with the CSR to acquire the records as if they are the actual customer. Our carrier investigations confirm that these calls are rebuffed, but these data brokers are quite determined. The data broker will scour other sources on the Internet or elsewhere to obtain my Social Security number or date of birth so that eventually the data broker will appear to be *Steve Largent* calling customer service, and thus, the CSR is duped into releasing the records. To be clear, from the carrier perspective, the CSR is dealing with the actual customer.

Make no mistake, these data thieves are extremely sophisticated. If they are unable to deceive one CSR on the first attempt, they will place multiple calls to customer service call centers until they are able to mislead a CSR into providing the call records.

No combination of identifiers is safe against pretexting. We have had cases where the data brokers have possessed the customer password. We have had cases where they knew the date of birth of the customer and the full Social Security number. Because many of these cases seem to arise in divorce or domestic cases, it is common for a spouse to have all of the necessary identifying information long after a divorce or separation to obtain call records.

WIRELESS CARRIER SECURITY PRACTICES

CTIA's members are committed to protecting customer privacy and security. This is no hollow pronouncement – we are talking about carriers protecting the privacy of their most valuable assets – their customers – as well as the very infrastructure of their networks. No carrier has an interest in seeing customer records disclosed without authority and every carrier has security policies and technical defenses to guard against it. I am also confident that our carriers are utilizing the best industry practices for combating fraud and ensuring security; however, the thieves who want to commit these crimes are constantly changing their tactics and approaches – staying one step ahead of them requires flexibility.

Wireless carriers employ a broad range of security measures beyond those put in place to meet the Federal Communications Commission's (FCC) customer proprietary network information (CPNI) rules to prevent unauthorized access to and disclosure of CPNI. I would note that no two carriers can or should employ the exact same security procedures. I would caution Committee members that as you proceed forward in drafting legislation that you consider the threat environment is constantly changing and static rules can quickly become outmoded or easily avoided by the fraudster. Additionally, CTIA in its comments to the EPIC petition for rulemaking at the FCC, noted that requiring wireless carriers to identify security procedures on the record and to further identify any inadequacies in those procedures would provide a roadmap to criminals to avoid fraud detection measures. Public disclosure potentially could lead to serious harm to consumers and carriers alike.

CPNI is protected from unauthorized disclosure under Section 222 of Title 47 and the FCC's implementing rules. "Every telecommunications carrier has a duty to

protect the confidentiality of proprietary information." Every wireless carrier takes that duty seriously; it is the law. The FCC, too, has followed up strongly on that mandate. In its very first order after the passage of the Telecommunications Act of 1996, the FCC directly addressed security concerns related to the protection of CPNI, and it has addressed the CPNI rules multiple times over.

Consistent with Congress's intent in Section 222, the wireless industry has worked continuously to maintain and improve the security of its customers' private information. CSRs are trained extensively on the rules related to access, use and disclosure of call records. Technical restrictions are placed on access to call records to ensure that no one can walk off with a data base of customer information, and CSRs are monitored to ensure they follow the necessary procedures. While we have heard stories about insiders selling call records on the side, we have not actually seen these cases. Instead, the vast majority of cases we have seen involve pretexting where the fraudster actually has all the necessary customer information to obtain the records.

Wireless carriers have taken additional measures to reiterate to their customers that it is important to continue to take steps to protect their accounts by utilizing passwords. For example, T-Mobile "urges all users of mobile services to take the following password protection steps:"

- create separate passwords for voicemail, online access, and for use when calling customer care about your billing account
- set complex passwords using both numbers and letters where appropriate

- avoid common passwords such as birthdates, family or pet names and street addresses
- change your passwords at least every 60 days
- memorize your passwords; and
- don't share passwords with anyone

But passwords get lost or forgotten and in many cases, customers call a CSR to refresh a password. The ability to change a password remotely presents another pretexting opportunity. In short, passwords are not a "silver bullet." Some carriers also report that some customers rebel against mandatory passwords, preferring instead to be empowered to make that choice individually, rather than by dictate.

The Committee should be aware that carriers are extremely cautious when allowing any third party vendor access to call records. Carrier contracts contain strict confidentiality and security provisions. It is common for carriers, for example, to require that vendors represent and warrant that they have adequate security procedures to protect customer information and to provide immediate notice of any security breach to the carrier. This contractual framework flows down a carrier's own security standards to vendors who conduct customer billing responsibilities creating security in depth.

One security practice we know now works is litigation. I cannot emphasize enough how seriously wireless carriers are taking these illegal and unauthorized attempts to obtain and traffic our customers' private information. These internal investigations have led to the carriers filing these cases which began months before the current media glare. As I mentioned at the beginning of my testimony, the four

national carriers: Verizon Wireless, Cingular, Sprint Nextel, and T-Mobile have all filed complaints and obtained injunctions across the country to shut these data thieves down. Moreover, smaller Tier II and Tier III wireless carriers are re-examining their security protocols to ensure their customers' privacy. The carriers' internal investigations against the data brokers made it possible to secure injunctions aimed at taking down the sites and preserving evidence so we can determine exactly who is buying the records through these brokers. We look forward to working with the Committee to utilize this information so Congress will be in a better position to draft legislation aimed not only at those who engage in pretexting, but also those that solicited the deed in the first place and later received the stolen property.

CUSTOMER SERVICE PROTECTIONS

As I mentioned previously, carriers have taken additional security steps to require personal identification numbers and passwords when obtaining call record information. For example, when call records are accessed, it is logged in the customer service database, so the carrier can see who looked at what records. Further, CSRs are trained to annotate the customer record whenever an account change or event occurs. A CSR will note when a customer called and asked for his or her records. To prevent the fraudster from adding a fax or email account identifier to another's account, many carriers have instituted a ban on faxing or e-mailing call records. It is important to remember, carriers are under tremendous pressure to quickly respond to customer calls. What was largely perceived as good customer service yesterday, is now a practice seen as a potential security flaw.

Because of the highly competitive nature of the wireless phone industry, customer service is extremely important to wireless carriers and their customers. Wireless carriers collectively received hundreds of millions, if not billions, of customer inquiries in 2005. Inside our member companies, CSRs are striving to address the requests of customers as best they can with the very best interest of the customer at heart. Bearing this statistic in mind, it could prove counter productive to enact legislation that would impede wireless customers' access to their own account information. Rules that may require in-person customer service would be a step backwards from the convenient and responsive customer service wireless carriers strive to achieve.

CONCLUSION

Clearly, the privacy of a small percentage of our customers and your constituents' has been compromised. As far as I am concerned, the breach of even one wireless customer's calling records, is one customer too many. But to the best of my knowledge no system is foolproof, especially one that handles hundreds of millions of customer calls each year without the customer being present.

The wireless industry wholeheartedly supports making it explicitly clear that the marketing, possession, and sale of call records is against the law. CTIA and its carriers are on record as supporting Congress's efforts to enact federal legislation that criminalizes the fraudulent behavior by third parties to obtain, sell, or distribute call records. Carriers have been successful in using existing state and federal law to obtain injunctions to shut down these Internet sites.

If we have learned anything from this experience, it is that combating pretexting is a war where the unscrupulous continuously seek out vulnerabilities and weaknesses in the carrier defenses. Unfortunately, no defense will be perfect, which is why we need a good offense and strong enforcement measures against these criminals.

In closing, I echo Chairman Barton's sentiment that "(w)hile businesses have legitimate reasons to compile and keep the data that define our lives, they have a responsibility to safeguard it as if it were their own."

Again, thank you for this opportunity and I welcome any questions you may have.